(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－264595
（P2003－264595A）
(43)公開日　平成15年９月19日(2003.9.19)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'（参考）
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　12/66	Ｂ　５Ｋ０３０
12/56	１００	12/56	１００Ｚ

審査請求　未請求　請求項の数13　ＯＬ　（全 15 頁）

(21)出願番号　特願2002－63993(P2002－63993)

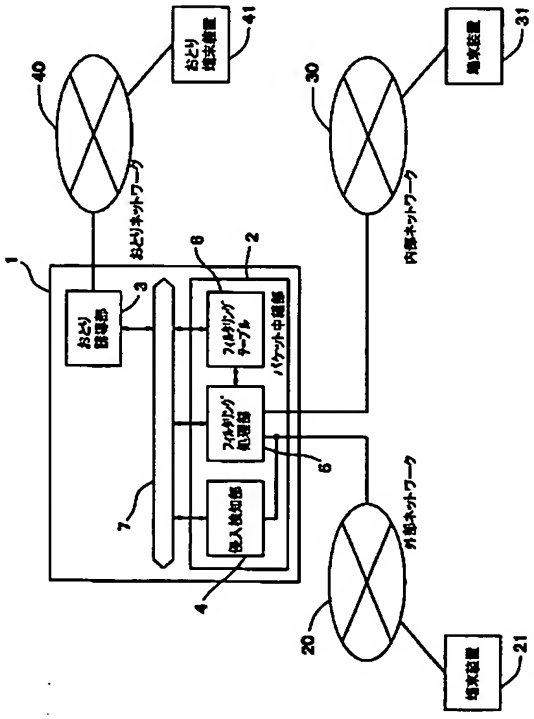
(22)出願日　平成14年３月８日(2002.3.8)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　木下　洋輔
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100073759
弁理士　大岩　増雄　（外３名）

Ｆターム(参考)　5K030 GA15 HA08 HD01 HD06 KA05 LB05

(54)【発明の名称】　パケット中継装置、パケット中継システムおよびオトリ誘導システム

(57)【要約】
【課題】　不正アクセスパケット又はその疑いのあるパケットをオトリネットワークへ送出することにより、不正アクセスに対するセキュリティ性を向上させたパケット中継装置を提供することを目的の一つとする。
【解決手段】　ネットワーク２０，３０間でパケットを中継するパケット中継部２と、ネットワーク２０からのパケットをオトリネットワーク４０へ送出するオトリ誘導部３とを備え、パケット中継部２が、フィルタリングテーブル６を用いて、ネットワーク２０からのパケットの破棄又はオトリ誘導を決定するフィルタリング処理部５と、ネットワーク２０からのパケットを監視してフィルタリングテーブル６を更新する侵入検知部とを有する。



1

【特許請求の範囲】

【請求項１】　第１のネットワークおよび第２のネットワーク間でパケットを中継するパケット中継部と、第１のネットワークから第２のネットワークに対して送信されたパケットを第１および第２のネットワークとは別のオトリネットワークへ送出するオトリ誘導部とを備え、

上記パケット中継部が、破棄すべきパケット又はオトリ誘導すべきパケットの送信元又は送信先情報を記憶するフィルタリングテーブルと、

フィルタリングテーブルを用いて、第１のネットワークから第２のネットワークに対して送信されたパケットの送信元又は送信先情報に基づき、当該パケットの破棄又はオトリ誘導を決定するフィルタリング処理部と、

第１のネットワークから第２のネットワークに対して送信されたパケットを監視して、第２のネットワークへ不正にアクセスしようとする不正アクセスパケットを検出し、フィルタリングテーブルを更新する侵入検知部とを有することを特徴とするパケット中継装置。

【請求項２】　上記オトリネットワークは、第２のネットワークと同一のア

ドレス体系を有するとともに、オトリ端末装置が接続され、

上記オトリ誘導部は、オトリ誘導されるパケットの送信先アドレス情報に一致する第１のアドレス情報が割り当てられたオトリ端末装置に対してパケットを送出することを特徴とする請求項１に記載のパケット中継装置。

【請求項３】　上記侵入検知部は、第１のネットワークから第２のネットワークに対して送信されたパケットを所定の不正アクセスパケットのパターンデータと比較して、不正アクセスパケットを検出することを特徴とする請求項１に記載のパケット中継装置。

【請求項４】　上記オトリ誘導部は、オトリ端末装置から第１のネットワークに対して送信されたパケットをパケット中継部へ送出し、

パケット中継部は、オトリ端末装置からのパケットを第１のネットワークへ送出することを特徴とする請求項１又は２に記載のパケット中継装置。

【請求項５】　上記オトリ誘導部は、オトリネットワークに接続された汎用コンピュータにより構成され、その汎用データバスを介してパケット中継部に接続され、

上記パケット中継部は、オトリ誘導部から受信したオトリネットワークから第１のネットワークに対して送信されたパケットに対し、フレーム形式を第２のネットワークの形式に変換して第１のネットワークに送出することを特徴とする請求項４に記載のパケット中継装置。

【請求項６】　上記オトリ誘導部は、オトリ端末装置から第１のネットワークに対して送信されたパケットについて、その送信先情報に基づき、オトリ誘導されたパケットの送信元以外を送信先とするパケットを判別し、判別されたパケットの送信元情報をオトリ端末装置に割り

2

当てられた第２のアドレスに変更してパケット中継部へ送出することを特徴とする請求項２に記載のパケット中継装置。

【請求項７】　上記パケット中継部は、第１のネットワークから送信されるパケットについて、第２のアドレスを送信先情報とするパケットを判別し、

上記オトリ誘導部が、判別されたパケットの送信先情報を第１のアドレスに変更して、オトリネットワークへ送出することを特徴とする請求項６に記載のパケット中継装置。

【請求項８】　請求項４に記載された第１および第２のパケット中継装置と、パケットを監視するパケット監視装置からなり、

第１のパケット中継装置の第１のネットワーク用のポートが第１のネットワークに接続され、

第２のパケット中継装置の第１のネットワーク用のポートが第２のネットワークに接続され、

第１および第２のパケット中継装置の第２のネットワーク用のポートが互いに接続され、正常パケットが伝送される第１の経路を形成し、

第１および第２のパケット中継装置のオトリネットワーク用のポートが互いに接続され、監視用経路として第１のパケット中継装置によってオトリ誘導されるべきパケットが伝送される第２の経路を形成し、

パケット監視装置が第２の経路に設けられることを特徴とするパケット中継システム。

【請求項９】　第１のネットワークおよび第２のネットワークに接続されたパケット中継装置と、第１および第２のネットワークとは別のオトリネットワークを介してパケット中継装置に接続されたオトリ端末装置とを備え、

パケット中継装置が、第１のネットワークおよび第２のネットワーク間でパケットを中継するパケット中継部と、第１のネットワークから第２のネットワークに対して送信されたパケットを第１および第２のネットワークとは別のオトリネットワークへ送出するオトリ誘導部とを有し、

上記パケット中継部が、破棄すべきパケット又はオトリ誘導すべきパケットの送信元又は送信先情報を記憶するフィルタリングテーブルと、

フィルタリングテーブルを用いて、第１のネットワークから第２のネットワークに対して送信されたパケットの送信元又は送信先情報に基づき、当該パケットの破棄又はオトリ誘導を決定するフィルタリング処理部と、

第１のネットワークから第２のネットワークに対して送信されたパケットを監視して、第２のネットワークへ不正にアクセスしようとする不正アクセスパケットを検出し、フィルタリングテーブルを更新する侵入検知部とを有することを特徴とするオトリ誘導システム。

【請求項１０】　上記パケット中継装置は、第１のネッ

トワークから第２のネットワークへの通信量が所定の閾値を越える場合に、第１のネットワークからのパケットをオトリ端末装置へ送出し、

上記オトリ端末装置は、パケット中継装置からの上記パケットを記録し、第１のネットワークから第２のネットワークへの通信量の低減後に第２のネットワークに対し送信することを特徴とする請求項９に記載のオトリ誘導システム。

【請求項１１】　上記オトリ端末装置は、オトリ誘導されたパケットのパケット情報を解析し、この解析結果に基づいて、オトリ誘導されたパケットを第２のネットワーク又は身代わり端末装置に対して送信することを特徴とする請求項９に記載のオトリ誘導システム。

【請求項１２】　上記パケット中継装置は、第１のネットワークから第２のネットワークに対して送信されたパケットを第２のネットワークおよびオトリ端末装置へ送出し、

オトリ端末装置が、オトリ誘導されたパケットのパケット情報を解析し、この解析結果に基づいて、第２ネットワークの監査を行うことを特徴とする請求項９に記載のオトリ誘導システム。

【請求項１３】　上記オトリ端末装置は、オトリ誘導されたパケットのパケット情報を解析し、この解析結果に基づいて、セッションリセットパケットを第１のネットワークに対して送出することを特徴とする請求項９に記載のオトリ誘導システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、パケット中継装置およびオトリ誘導システムに係り、更に詳しくは、侵入検知機能とネットワーク中継機能とを連携させるとともに、外部ネットワークからのパケットをオトリネットワークへ誘導することができるパケット中継装置、並びに、これを用いたパケット中継システムおよびオトリ誘導システムに関する。

【０００２】

【従来の技術】図１３は、従来の侵入検知システムの構成および動作を示した図である。図中の１はパケット中継装置、２０は外部ネットワーク、２１は外部端末装置、３０は内部ネットワーク、３１は内部端末装置、５０は管理者端末、５１は解析装置である。

【０００３】パケット中継装置１は、外部ネットワーク２０および内部ネットワーク３０に接続され、両ネットワーク間での通信されるパケットの中継を行っている。すなわち、外部端末装置２１から内部端末装置３１へのパケットを外部ネットワーク２０から受信し、内部ネットワーク３０へ送出する。また、内部端末装置３１から外部端末装置２１へのパケットを内部ネットワーク３０から受信し、外部ネットワーク２０へ送出する。

【０００４】ここで、外部ネットワーク２０から内部ネットワーク３０へのアクセスは制限されている場合がある。例えば、ＩＤコード及びパスワードによって認証された者だけが内部端末装置３１にアクセスすることが出来るような場合である。この様な場合、外部ネットワーク２０から内部ネットワーク３０へ不正にアクセスしようとする攻撃者からのパケット、つまり、不正アクセスパケットが送られてくることがある。

【０００５】このような不正アクセスから内部ネットワークを防御するため、一般に、パケット中継装置１は、不正アクセスパケットを検出するためのフィルタリング機能を有している。このようなパケット中継装置は、不正アクセスパケットの送信元又は送信先情報が規定されたフィルタリングテーブルを用いて、外部ネットワーク２０からの不正アクセスパケットを判別し、不正アクセスパケットであることが判別できれば、当該パケットは内部ネットワーク３０へ送出されない。

【０００６】この様なフィルタリング機能を有するパケット中継装置においては、フィルタリングテーブルの内容が重要であり、内部ネットワーク３０のセキュリティを高めるために、一元的なポリシー（特定のデータを受信すれば通信を遮断する等の極端なポリシー）を設定したとすれば、不正アクセスは排除することができるが、ネットワークの可用性を確保することが困難になる。このため、運用時に、ネットワーク管理者が、不正アクセスの疑いのある被疑パケット１つ１つについて不正アクセスパケットであるか否かを判断し、フィルタリングテーブルを更新していく必要がある。

【０００７】解析装置５１は、パケット中継装置１および内部ネットワーク３０を監視し、通信データの記録等を行うことによって、外部ネットワーク２０から内部ネットワーク３０への不正アクセス検知の手掛かりとなる情報を収集する。収集された情報は、解析装置５１において解析され、ネットワーク管理者の管理者端末装置５０へ通知される。

【０００８】ネットワーク管理者は、管理者端末装置５０を用いて、パケット中継装置１のフィルタリングテーブルを設定し、更新することができる。ネットワーク管理者は、解析装置５１による解析結果に基づき、不正アクセスパケットおよび不正アクセスの疑いのあるパケットであるか否かの最終的な判断を行い、フィルタリングテーブルをを変更し、不正アクセスの再発を防止している。

【０００９】

【発明が解決しようとする課題】従来の侵入検知システムは上記のように構成され、ネットワーク管理者によって管理されていた。ところが、このようなネットワーク管理業務は、専門知識を有するスペシャリストのみが行うことのできる業務であるため、一部の管理者に大きな作業負荷が集中してしまうという問題があった。

【００１０】また、パケット中継装置は、ＩＤＳ（Intr

usion Detection System）と呼ばれる侵入検知機能を有している場合がある。ＩＤＳを用いれば、パケットデータのパターンマッチングにより、不正アクセスパケットを判別することができる。しかしながら、パケット単位のパターンマッチングだけでは不正アクセスパケットであると判断できない様な場合、内部ネットワークに不正アクセスパケットが送出されてしまうという問題があった。また、ＩＤＳによる不正アクセスパケットの検出には時間がかかるため、パケット通信量が多い場合には、全てのパケットについて判断を行うことができないという問題もあった。

【００１１】本発明は、上記の事情に鑑みてなされたものであり、セキュリティ機能を有するパケット中継装置であって、不正アクセスパケット又はその疑いのあるパケットをオトリネットワークへ送出することにより、不正アクセスに対するセキュリティ性を向上させ、あるいは、不正アクセスへの対処を自動化したパケット中継装置を提供することを目的とする。また、通信量の増大時にパケットをオトリネットワークへ送出することにより、通信路の帯域を確保するパケット中継装置を提供することを目的とする。

【００１２】また、セキュリティ機能を有するパケット中継システムであって、２つの中継経路を用いて、中継経路における帯域を制御し、セキュリティ性を向上させたパケット中継システムを提供することを目的とする。

【００１３】また、セキュリティ機能を有するパケット中継装置および不正アクセスパケット又はその疑いのあるパケットがオトリネットワークを介して誘導されるオトリ端末装置からなるオトリ誘導システムを提供することを目的とする。さらに、セキュリティレベルを変化させ、ネットワークの監査を行い、あるいは、不正アクセスへの対処をリアルタイム化したオトリ誘導システムを提供することを目的とする。

【００１４】

【課題を解決するための手段】請求項１に記載の本発明によるパケット中継装置は、第１のネットワークおよび第２のネットワーク間でパケットを中継するパケット中継部と、第１のネットワークから第２のネットワークに対して送信されたパケットを第１および第２のネットワークとは別のオトリネットワークへ送出するオトリ誘導部とを備えて構成される。

【００１５】上記パケット中継部は、破棄すべきパケット又はオトリ誘導すべきパケットの送信元又は送信先情報を記憶するフィルタリングテーブルと、フィルタリングテーブルを用いて、第１のネットワークから第２のネットワークに対して送信されたパケットの送信元又は送信先情報に基づき、当該パケットの破棄又はオトリ誘導を決定するフィルタリング処理部と、第１のネットワークから第２のネットワークに対して送信されたパケットを監視して、第２のネットワークへ不正にアクセスしようとする不正アクセスパケットを検出し、フィルタリングテーブルを更新する侵入検知部とにより構成される。

【００１６】請求項２に記載の本発明によるパケット中継装置は、オトリネットワークが、第２のネットワークと同一のアドレス体系を有するとともに、オトリ端末装置が接続される。また、オトリ誘導部が、オトリ誘導されるパケットの送信先アドレス情報に一致する第１のアドレス情報が割り当てられたオトリ端末装置に対してパケットを送出するように構成される。

【００１７】請求項３に記載の本発明によるパケット中継装置は、侵入検知部が、第１のネットワークから第２のネットワークに対して送信されたパケットを所定の不正アクセスパケットのパターンデータと比較して、不正アクセスパケットを検出するように構成される。

【００１８】請求項４に記載の本発明によるパケット中継装置は、オトリ誘導部が、オトリ端末装置から第１のネットワークに対して送信されたパケットをパケット中継部へ送出し、パケット中継部が、オトリ端末装置からのパケットを第１のネットワークへ送出するように構成される。

【００１９】請求項５に記載の本発明によるパケット中継装置は、オトリ誘導部が、オトリネットワークに接続された汎用コンピュータにより構成され、その汎用データバスを介してパケット中継部に接続され、パケット中継部が、オトリ誘導部から受信したオトリネットワークから第１のネットワークに対して送信されたパケットに対し、フレーム形式を第２のネットワークの形式に変換して第１のネットワークに送出するように構成される。

【００２０】請求項６に記載の本発明によるパケット中継装置は、オトリ誘導部が、オトリ端末装置から第１のネットワークに対して送信されたパケットについて、その送信先情報に基づき、オトリ誘導されたパケットの送信元以外を送信先とするパケットを判別し、判別されたパケットの送信元情報をオトリ端末装置に割り当てられた第２のアドレスに変更してパケット中継部へ送出するように構成される。

【００２１】請求項７に記載の本発明によるパケット中継装置は、パケット中継部が、第１のネットワークから送信されるパケットについて、第２のアドレスを送信先情報とするパケットを判別し、オトリ誘導部が、判別されたパケットの送信先情報を第１のアドレスに変更して、オトリネットワークへ送出するように構成される。

【００２２】請求項８に記載の本発明によるパケット中継システムは、第１および第２のパケット中継装置と、パケットを監視するパケット監視装置により構成される。第１のパケット中継装置の第１のネットワーク用のポートが第１のネットワークに接続され、第２のパケット中継装置の第１のネットワーク用のポートが第２のネットワークに接続され、第１および第２のパケット中継装置の第２のネットワーク用のポートが互いに接続さ

れ、正常パケットが伝送される第１の経路を形成し、第１および第２のパケット中継装置のオトリネットワーク用のポートが互いに接続され、監視用経路として第１のパケット中継装置によってオトリ誘導されるべきパケットが伝送される第２の経路を形成し、パケット監視装置が第２の経路に設けられる。

【００２３】請求項９に記載の本発明によるオトリ誘導システムは、第１のネットワークおよび第２のネットワークに接続されたパケット中継装置と、第１および第２のネットワークとは別のオトリネットワークを介してパケット中継装置に接続されたオトリ端末装置とを備えて構成される。

【００２４】上記パケット中継装置は、第１のネットワークおよび第２のネットワーク間でパケットを中継するパケット中継部と、第１のネットワークから第２のネットワークに対して送信されたパケットを第１および第２のネットワークとは別のオトリネットワークへ送出するオトリ誘導部とにより構成される。

【００２５】上記パケット中継部は、破棄すべきパケット又はオトリ誘導すべきパケットの送信元又は送信先情報を記憶するフィルタリングテーブルと、フィルタリングテーブルを用いて、第１のネットワークから第２のネットワークに対して送信されたパケットの送信元又は送信先情報に基づき、当該パケットの破棄又はオトリ誘導を決定するフィルタリング処理部と、第１のネットワークから第２のネットワークに対して送信されたパケットを監視して、第２のネットワークへ不正にアクセスしようとする不正アクセスパケットを検出し、フィルタリングテーブルを更新する侵入検知部とにより構成される。

【００２６】請求項１０に記載の本発明によるオトリ誘導システムは、パケット中継装置が、第１のネットワークから第２のネットワークへの通信量が所定の閾値を越える場合に、第１のネットワークからのパケットをオトリ端末装置へ送出し、オトリ端末装置が、パケット中継装置からの上記パケットを記録し、第１のネットワークから第２のネットワークへの通信量の低減後に第２のネットワークに対し送信するように構成される。

【００２７】請求項１１に記載の本発明によるオトリ誘導システムは、オトリ端末装置が、オトリ誘導されたパケットのパケット情報を解析し、この解析結果に基づいて、オトリ誘導されたパケットを第２のネットワーク又は身代わり端末装置に対して送信するように構成される。

【００２８】請求項１２に記載の本発明によるオトリ誘導システムは、パケット中継装置が、第１のネットワークから第２のネットワークに対して送信されたパケットを第２のネットワークおよびオトリ端末装置へ送出し、オトリ端末装置が、オトリ誘導されたパケットのパケット情報を解析し、この解析結果に基づいて、第２ネットワークの監査を行うように構成される。

【００２９】請求項１３に記載の本発明によるオトリ誘導システムは、オトリ端末装置が、オトリ誘導されたパケットのパケット情報を解析し、この解析結果に基づいて、セッションリセットパケットを第１のネットワークに対して送出するように構成される。

【００３０】

【発明の実施の形態】実施の形態１．図１は、本発明の実施の形態１によるオトリ誘導システムの一構成例を示したブロック図である。図中の１はオトリ誘導装置、２はパケット中継部、３はオトリ誘導部、４は侵入検知部、５はフィルタリング処理部、６はフィルタリングテーブル、７は内部バス、２０は外部ネットワーク、２１は外部端末装置、３０は内部ネットワーク、３１は内部端末装置、４０はオトリネットワーク、４１はオトリ端末装置である。

【００３１】オトリ誘導装置１は、外部ネットワーク２０および内部ネットワーク３０に接続され、両ネットワーク間でパケット中継を行うパケット中継装置である。すなわち、外部端末装置２１から内部端末装置３１へのパケットを外部ネットワーク２０から受信し、内部ネットワーク３０へ送出する。また、内部端末装置３１から外部端末装置２１へのパケットを内部ネットワーク３０から受信し、外部ネットワーク２０へ送出する。

【００３２】各ネットワーク２０，３０，４０には、通常、２以上の端末装置が接続されているが、図中では省略されている。特に、外部ネットワーク２０は、インターネットのような不特定多数の端末装置が収容されているネットワークであってもよい。オトリネットワーク４０は、内部ネットワーク３０には接続されてない（オトリ誘導装置１経由を除く）別個のネットワークであり、オトリ端末装置４１が接続されている。

【００３３】オトリ誘導装置１は、外部ネットワーク２０および内部ネットワーク３０に接続されたパケット中継部２と、オトリネットワーク４０に接続されたオトリ誘導部３からなり、パケット中継部２およびオトリ誘導部３は、内部バス７を介して接続されている。パケット中継部２は、さらに侵入検知部４と、フィルタリング処理部５と、フィルタリングテーブル６とにより構成される。

【００３４】オトリ誘導部３、侵入検知部４およびフィルタリング処理部５は、ネットワーク経路（外部ネットワーク２０，内部ネットワーク３０）以外のパスである内部バス７を介して互いに通信することができる。また、オトリ誘導部３および侵入検知部４は、ネットワーク中継機能を利用するユーザからは隠蔽されている。

【００３５】侵入検知部４は、外部ネットワーク２０からのパケットのステルス監視を行って、ＤｏＳ（Denial of Service）、スキャニングなどのネットワークレベルの攻撃（不正アクセス）を検出している。例えば、監視対象であるパケットデータを予め与えられた不正パケ

ットパターンと比較して、不正アクセスパケットを検出する。このパターンマッチングは、パケット単位だけでなく、送信元又は送信先情報によって特定される一連のパケットに対して行うこともできる。

【００３６】フィルタリング処理部５は、外部ネットワーク２０から送信されたパケットに対し、内部ネットワーク３０への中継、オトリネットワーク４０への誘導、破棄のいずれかの処理（フィルタリング処理）を行っている。この処理は、フィルタリングテーブルに基づいて行われ、例えば、内部ネットワーク３０に不正にアクセスしようとする不正アクセスパケットは破棄され、不正アクセスの疑いのある被疑パケットはオトリネットワーク４０へ誘導され、その他の通常パケットは、内部ネットワーク３０へ送出される。

【００３７】フィルタリングテーブル６には、フィルタリング処理を規定するデータが記憶されており、パケットヘッダに含まれる送信元又は送信先に関する情報と、当該パケットに対するフィルタリング処理とが関連づけられている。たとえば、破棄すべきパケットおよびオトリ誘導すべきパケットとして、パケットの送信元又は送信先情報が記憶されており、送信元又は送信先情報がフィルタリングテーブル６と一致するパケットは、破棄され、あるいは、オトリ誘導される一方、その他のパケットはネットワーク中継される。このフィルタリングテーブル６は、侵入検知部４による検出結果に基づいて更新される。

【００３８】オトリ誘導部３は、内部バス７を介して、フィルタリング処理部５から、オトリ誘導すべきパケットを受信し、オトリネットワーク４０上のオトリ端末装置４１へ送出する。

【００３９】次に動作について説明する。外部端末装置２１から内部端末装置３１に対して送信されたパケットは、外部ネットワーク２０を介してオトリ誘導装置１により受信される。この受信パケットは、パケット中継部２のフィルタリング処理部５へ入力されるとともに、侵入検知部４にも入力される。この侵入検知部４は、パケット中継部２の入り口でプロミスカスモードかつステルスモードで通信を傍受している。

【００４０】パケットを受信したフィルタリング処理部５は、フィルタリングテーブル６に基づいて、送信元又は送信先情報、例えば、送信元ＩＰ（Internet Protocol）アドレス、送信先ＩＰアドレス、送信元ＴＣＰ（Transmission Control Protocol）ポート番号、送信先ＴＣＰポート番号、送信元ＵＤＰ（User Datagram Protocol）ポート番号または送信先ＵＤＰポート番号をチェックする。

【００４１】この結果、フィルタリングテーブル６において、破棄の指定がされているパケットは、フィルタリング処理部５によって破棄され、オトリ誘導の指定がされているパケットがオトリサイト（オトリネットワーク４０のオトリ端末装置４１）へ誘導され、ともに内部ネットワーク３０には送出されない。一方、破棄および誘導等の指定がされていないパケットは内部ネットワーク３０へ送出される。

【００４２】図２は、図１のオトリ誘導システムにおけるパケットの流れの一例を示した図である。外部ネットワーク２０から内部ネットワーク３０に対して送信されたパケットは、フィルタリングテーブル６に基づいて、破棄され、オトリネットワーク４０へオトリ誘導され、あるいは、内部ネットワーク３０へ中継される。

【００４３】一方、パケットを傍受した侵入検知部４は、所定の不正アクセスパターンによりパターンマッチングを行って、傍受したパケットが不正アクセスパケットかどうかを判別する。不正アクセスパケットを受信した場合、あらかじめ定められたポリシー（不正アクセスの種類とそれに対する対策の関係）に従って、送信元又は送信先情報と、それに関連づけられるフィルタリング処理（破棄又は誘導）を決定し、内部バス７を介してフィルタリング処理部５へ通知し、フィルタリングテーブル６が更新される。

【００４４】例えば、不正アクセスが疑われるパケットが検出された場合には、当該パケットがオトリ誘導の対象に追加され、不正アクセスパケットであることが検出された場合には、破棄の対象に追加される。逆に、オトリ誘導又は破棄の対象が、正常アクセスパケットであることが検出された場合には、これらの対象から除外される。この様なポリシーは予め任意に決定され、侵入検知部４に対し与えられている。

【００４５】本実施の形態によれば、侵入検知部４によって外部ネットワーク２０からの不正アクセスパケットが検出され、フィルタリングテーブル６が自動的に更新されるため、フィルタリングポリシーをダイナミック（動的）に自動変更させることができる。このため、不正アクセスパケットに応じた対策をリアルタイムで実現し、セキュリティ性を向上させることができる。

【００４６】また、外部ネットワーク２０から内部ネットワーク３０へのパケットのうち、不正アクセスの疑いのあるパケットをオトリ端末装置４１に誘導することによって、内部ネットワーク３０への不正アクセスを未然に防止することができる。

【００４７】実施の形態２．図３は、本発明の実施の形態２によるオトリ誘導システムの一構成例を示したブロック図である。図中の８はパーソナルコンピュータ、９はアドインボード、１０はＰＣＩ（Peripheral Components Interconnect）バス、１１はＰＣＩインターフェース部、１２はＴＣＰ／ＩＰインターフェース部である。なお、図１に示されたブロックに相当するブロックには同一の符号を付して説明を省略する。

【００４８】パーソナルコンピュータ８は、オトリ誘導部３と、ＰＣＩインターフェース部１１と、ＴＣＰ／Ｉ

Ｐインターフェース部１２からなる。オトリ誘導部３は、汎用のパーソナルコンピュータ上で実行されるソフトウエアとして構成され、ＰＣＩインターフェース部１１を介してＰＣＩバス１０に接続され、アドインボード９との通信を行うとともに、ＴＣＰ／ＩＰインターフェース１２を介してオトリネットワーク４０に接続され、オトリ端末装置４１との通信を行うことができる。このパーソナルコンピュータ８は、アドインボード９とともにオトリ誘導装置を構成する。

【００４９】アドインボード９は、ＰＣＩバス１０を介してパーソナルコンピュータ８に接続されたパケット中継のための機器であり、パーソナルコンピュータ８の筐体内に組み込まれている。このアドインボード９は、侵入検知部４、フィルタリング処理部５およびフィルタリングテーブル６からなり、侵入検知部４およびフィルタリング処理部５がＰＣＩバス１０に接続されている。なお、ＰＣＩバス１０は、図１の内部バス７に相当し、アドインボード９は、図１のパケット中継部２に相当する。

【００５０】内部ネットワーク３０およびオトリネットワーク４０は、パーソナルコンピュータ８およびアドインボード９を介して、ＰＣＩバスにより接続されるのみであり、ネットワークとしては両者は完全に切り離されている。このため、オトリネットワーク４０の環境（例えばＩＰアドレス等のネットワーク設定情報）を内部ネットワーク３０の環境に限りなく近づけることができる。つまり、オトリネットワーク４０に、内部ネットワーク３０と同じプロトコルやアドレス体系を採用し、さらに、内部ネットワーク３０上の端末装置３１と同じＩＰアドレスをオトリネットワーク４０上のオトリ端末装置４１に割り当てることができる。

【００５１】不正アクセスを試みる外部ネットワーク２０上の利用者（攻撃者）は、オトリ端末装置４１との通信により、オトリ端末装置４１からアクセス可能な様々な情報を取得できる可能性がある。このため、両ネットワーク３０，４０の環境を近づければ、不正アクセスパケットをオトリサイトに誘導した場合に、オトリ誘導していることを攻撃者に気づかれ難くすることができる。

【００５２】次に動作について説明する。図４は、図３のオトリ誘導システムの通常運用時の動作の一例を示した図である。通常運用時のパケットの流れは、実施の形態１と同様にパケット中継部としてのアドインボード９を介して行われる。すなわち、　外部ネットワーク２０からのパケットは、フィルタリング処理部５に入力され、破棄、オトリ誘導の対象でないパケットは、内部ネットワーク３０へ送出される。　侵入検知部４は、アドインボード９の入り口でパケットを傍受し、不正アクセスかどうかの判断を行う。　不正アクセスを発見した場合、それ以降の不正アクセスを未然に防ぐために、ＰＣＩバスを介してフィルタリングテーブル６を更新し、中継ポリシーを自動的に変更する。

【００５３】図５は、図３のオトリ誘導システムにおいて、フィルタリング処理部によってパケットがオトリ誘導される場合の動作の一例を示した図である。　外部ネットワーク２０からパケットを受信したフィルタリング処理部５は、フィルタリングテーブル６に従って、送信元又は送信先情報、例えば、送信元ＩＰアドレス、送信先ＩＰアドレス、送信元ＴＣＰポート番号、送信先ＴＣＰポート番号、送信元ＵＤＰポート番号または送信先ＵＤＰポート番号をチェックする。この結果、オトリ誘導が指定されたパケットであれば、オトリ端末装置４１へ誘導するため、当該パケットをＰＣＩバス１０を通じてパーソナルコンピュータ８へ転送する。　パーソナルコンピュータ上のプログラムとしてのオトリ誘導部３はパケットの種別を判断し、オトリ端末装置４１が受信可能なパケット形式に変換した後、当該パケットをオトリネットワーク４０へ送出する。

【００５４】なお、侵入検知部４が外部ネットワーク２０からの不正アクセスを検出した場合には、侵入検知部４からフィルタリング処理部５へ攻撃検知の通知が送られ、フィルタリング処理部５は内部ネットワーク３０への当該通信を一旦遮断する。このとき、上述した通り、フィルタリングテーブル６が更新されるので、その後に受信した同種のパケットは、フィルタリング処理部５によってオトリ端末装置４１へ誘導される。

【００５５】一方、オトリ端末装置４１が、外部ネットワーク２０上の外部端末装置２１（攻撃者）に対しパケットを送信する場合、　オトリ端末装置４１からのパケットは、オトリネットワーク４０を介してパーソナルコンピュータ８に入力される。当該パケットをＴＣＰ／ＩＰインターフェース１２を介して受け取ったオトリ誘導部３は、ＰＣＩバス１０を介してアドインボード９へパケットの転送要求を出す。　ＰＣＩバス１０を介してパケットの転送要求を受け取ったフィルタリング処理部５は、受信したパケットデータをイーサネット（登録商標）フレームの形式に変換（イーサフレーミング）して外部ネットワーク２０へ送出する。

【００５６】本実施の形態では、オトリ誘導部３をパーソナルコンピュータ８上のソフトウエアにより実現し、当該コンピュータにパケット中継装置としてのアドインボード９をＰＣＩバス１０により接続しているため、ＰＣＩドライバを開発すれば、既存のパーソナルコンピュータを使用して、オトリ誘導システムを構築することができる。

【００５７】また、オトリ端末装置４１からのパケットを外部ネットワーク２０に送出し、内部ネットワーク３０上の端末装置３１からのパケットに見せかけているため、不正アクセスを試みる外部ネットワーク２０の利用者（攻撃者）にオトリ誘導されていることを気づかれ難

くなる。

【００５８】特に、オトリネットワーク４０のプロトコル、アドレス体系を内部ネットワーク３０のそれと同一とし、オトリ誘導される不正アクセスパケットをその送信先情報（つまり内部ネットワーク上の端末装置３１）と同じアドレス情報が割り当てられたオトリネットワーク４０上のオトリ端末装置４１に送出することにより、オトリ誘導に気づかれ難くすることができる。

【００５９】実施の形態３．実施の形態２では、オトリ端末装置４１から外部ネットワーク２０上の攻撃者へパケットを送信する場合について説明したが、本実施の形態では、オトリ端末装置４１と、外部ネットワーク２０上の攻撃者以外の端末装置との間でパケット通信を行う場合について説明する。

【００６０】各オトリ端末装置４１は、オトリ誘導部３により起動時に仮想的なＩＰアドレスが割り当てられる。オトリ誘導部３は、各オトリ端末装置４１に割り当てた仮想アドレスを本来のＩＰアドレスに対応づけて記憶するとともに、フィルタリング処理部５に対し、仮想アドレスを通知し、これらのアドレスを送信先としたパケットを受信した場合には、オトリ誘導部３に転送するように要求する。

【００６１】まず、オトリ端末装置４１が、外部ネットワーク２０上の攻撃者以外の端末装置、たとえばＤＮＳ（Domain Name Server）に対して、パケットを送信する場合について説明する。

【００６２】図６は、本発明の実施の形態３によるオトリ端末装置４１から攻撃者以外の外部端末装置にパケット送信する場合の動作を示した説明図である。オトリ端末装置４１には、オトリ誘導時に使用される本来のＩＰアドレスとして”10.255.0.1”が割り当てられ、仮想アドレスとして”10.0.0.1”が割り当てられているものとする。また、攻撃者以外の外部端末装置にはＩＰアドレス”w.x.y.z”が割り当てられているものとする。

【００６３】オトリ誘導装置１が、オトリ端末装置４１からのパケットを受信した場合、オトリ誘導部３が、そのパケットの送信先（destination：dst）アドレスを検査して、攻撃者宛でないかを判断する。その結果、攻撃者宛でない場合には、オトリ誘導部３が当該パケットの送信元（source：src）アドレス”10.0.0.1”を、当該オトリ端末装置４１に対して起動時に割り当てられた仮想アドレス”10.255.0.1”に変更する。このとき、ＩＰパケットのチェックサム（Checksum）を再計算し変更する必要がある。この様にして送信元アドレスが変更されたパケットは、ＰＣＩインターフェースを介してフィルタリング処理部５に送られ、オトリ誘導装置１からインターネットなどの外部ネットワーク２０へ送出される。

【００６４】次に、外部ネットワーク２０上の攻撃者以外の端末装置、たとえばＤＮＳからオトリ端末装置４１に対して、パケットが送信される場合について説明する。

【００６５】図７は、攻撃者以外の外部端末装置からオトリ端末装置４１に対してパケット送信する場合の動作を示した説明図である。図６と同様、オトリ端末装置４１には、本来のＩＰアドレスとして”10.255.0.1”が割り当てられ、仮想アドレスとして”10.0.0.1”が割り当てられているものとする。また、攻撃者以外の外部端末装置にはＩＰアドレス”w.x.y.z”が割り当てられているものとする。

【００６６】オトリ誘導装置１が外部ネットワーク２０からパケットを受信した場合、フィルタリング処理部５は、受け取ったパケットの送信先アドレスが、オトリ誘導部３から予め通知された仮想アドレス” 10.255.0.1”であるかを検査する。この結果、仮想アドレス宛のパケットであれば、そのパケットをオトリ誘導部３に転送する。オトリ誘導部３は、転送されたパケットの送信先情報を本来のＩＰアドレス”10.0.0.1”に変更し、チェックサムを再計算し変更する。この様にして送信先アドレスが変更されたパケットは、ＴＣＰ／ＩＰインターフェース１２を介してオトリネットワーク４０へ送出され、オトリ端末装置４１により受信される。

【００６７】実施の形態４．実施の形態１～３では、フィルタリング処理部５が受信パケットに基づいて判断し、その判断結果に基づいて、パケットをオトリ端末装置４１へ送信する動作について説明したが、本実施の形態では、図１，３のオトリ誘導システムにおいて、所定量を超えるパケット通信が発生した場合に、通信パケットの全て又は一部をオトリ端末装置４１に誘導する場合の動作について説明する。

【００６８】図８は、本発明の実施の形態４によるオトリ誘導システムの動作の一例を示した説明図である。通常運用時、外部ネットワーク２０から受信したパケットは、破棄又はオトリ誘導が指定されているパケットを除き、内部ネットワーク３０へ直接中継される。

【００６９】一方、　予め定められた閾値を超える通信が発生した場合、フィルタリング処理部５は、全ての通信または一部の通信（たとえば、特定の送信元ＩＰアドレス、特定の送信先ＩＰアドレス、特定の送信元ＴＣＰポート番号、特定の送信先ＴＣＰポート番号、特定の送信元ＵＤＰポート番号または特定の送信先ＵＤＰポート番号によって限定される）をオトリ端末装置４１へ誘導し、本来の通信路の帯域を確保する。このとき、オトリ端末装置４１では、誘導されてきたパケットをログ情報として蓄積する。

【００７０】　フィルタリング処理部５から通信量が減少した旨の通知を受けたオトリ端末装置４１は、蓄積しているログ情報をパケットに変換して、フィルタリング処理部５へ転送する。フィルタリング処理部５は、これらのパケットを内部ネットワーク３０へ送出する。

【００７１】本実施の形態によれば、所定の通信パケッ

トを一旦、オトリ端末装置４１に蓄積させることにより、特定の通信のための帯域を確保するとともに、ネットワークの負荷を分散させることができる。

【００７２】実施の形態５．実施の形態１～４では、外部ネットワークからのパケットをオトリ端末装置に誘導するオトリ誘導システムについて説明したが、本実施の形態では、これらのオトリ誘導システムにおいてオトリ誘導装置として使用されているパケット中継装置を２台連携させ、パケット中継システムとして動作させる場合について説明する。

【００７３】図９は、本発明の実施の形態５によるパケット中継システムの一構成例を示した図である。図中の１Ａ、１Ｂはパケット中継装置、１３はパケット中継システム、１４はパケット監視装置（sniffer）、１５は通常ルート、１６は監視ルートである。

【００７４】２つの同一のパケット中継装置１Ａ，１Ｂは、いずれも図１および図３においてオトリ誘導装置として示されたパケット中継装置であり、本実施の形態では、２個のパケット中継装置１Ａ，１Ｂおよびパケット監視装置１４によって、パケット中継システム１３を構成している。

【００７５】パケット中継システム１３は外部ネットワーク２０および内部ネットワーク３０に接続され、外部ネットワーク２０および内部ネットワーク３０間でのパケット中継を行っている。外部ネットワーク２０との接続にはパケット中継装置１Ａが使用され、内部ネットワーク３０との接続にはパケット中継装置１Ｂが使用され、両パケット中継装置１Ａ，１Ｂがパケット中継システム１３内で接続されている。

【００７６】すなわち、外部ネットワーク側のパケット中継装置１Ａは、図１，３における外部ネットワーク用ポートが、外部ネットワーク２０に接続され、内部ネットワーク側のパケット中継装置１Ｂは、図１，３における外部ネットワーク用のポートが内部ネットワーク３０に接続されている。また、パケット中継装置１Ａ，１Ｂは、図１，３における内部ネットワーク用のポートが互いに接続され、中継パケットの通常ルート１５を形成し、オトリネットワーク用のポートが互いに接続されて通信パケットの監視ルート１６を形成している。

【００７７】パケット監視装置１４は、パケット中継装置１Ａ，１Ｂ間の監視ルートに設けられ、当該ルートを通過するパケットの内容を監視している。各パケット中継装置１Ａ，１Ｂを構成する図１，３におけるオトリ誘導部３は、パケットを監視ルート１６へルート変更させる監視ルート誘導部となり、パケット監視装置１４は誘導されたパケットのみを対象としてパケットデータを詳細にチェックし、不正アクセスパケットであるか否かを判別する。

【００７８】次に動作について説明する。　通常運用時、全てのパケットが通常ルート１５に割り当てられ、監視ルート１６は使用されることなく、通常ルート１５経由でパケット中継が行われる。すなわち、外部ネットワーク２０からのパケットは、パケット中継装置１Ａにより通常ルート１５へ出力され、パケット中継装置１Ｂを介して内部ネットワーク３０へ送出される。同様にして、内部ネットワーク３０からのパケットは、パケット中継装置１Ｂにより通常ルート１５へ出力され、パケット中継装置１Ａを介して外部ネットワーク２０へ送出される。

【００７９】　不正アクセスの兆候のあるパケットが検出された場合、該当するパケットには監視ルート１６が割り当てられる。すなわち、パケット中継装置１Ａ，１Ｂのフィルタリング処理部５が、送信元又は送信先情報に基づいて、監視ルート１６に誘導すべきパケットを判別する。例えば、特定の送信元ＩＰアドレス、特定の送信先ＩＰアドレス、特定の送信元ＴＣＰポート番号、特定の送信先ＴＣＰポート番号、特定の送信元ＵＤＰポート番号または特定の送信先ＵＤＰポート番号により誘導すべきパケットがフィルタリングテーブルにより指定される。この様にして、判別されたパケットは、パケット中継装置１Ａ，１Ｂの監視ルート誘導部（オトリ誘導部）を介してを監視ルート１６へ出力され、パケット監視装置１４の監視対象となる。

【００８０】一般に、パケット監視装置１４がパケットデータを詳細にチェックしようとした場合、パケット監視装置１４の負荷が増大し、処理に要する時間が長くなる。このため、パケット通信量が多い場合には、全てのパケットについてリアルタイムでチェックすることが出来なくなる。

【００８１】本実施の形態によれば、特定のパケット、例えば不正アクセスの疑いのあるパケットのみを監視ルート１６へ誘導する経路の制御を行っている。このため、パケット監視装置１４は、帯域が制限された監視ルート１６上のパケットについてのみ監視を行うことにより、的確なパケット監視を確実に行うことが出来る。また、不正アクセス者に気づかれることなく、物理的に隔離して監視することができる。

【００８２】実施の形態６．実施の形態１～４では、外部ネットワークからのパケットをオトリ端末装置に誘導するオトリ誘導装置について説明したが、本実施の形態では、オトリ端末装置に加えて身代わり端末装置を備え、段階的に誘導してパケットに応じてセキュリティーレベルを異ならせるオトリ誘導システムについて説明する。

【００８３】図１０は、本発明の実施の形態６によるオトリ誘導システムの構成および動作の一例を示した図である。図中の１はパケット中継装置、２０は外部ネットワーク、３０は内部ネットワーク、４１はオトリ端末装置、４２は身代わり端末装置である。

【００８４】　通常運用時、外部ネットワーク２０から

のパケットは、内部ネットワーク３０へ直接中継される。　ある特定の通信（特定の送信元ＩＰアドレス、特定の送信先ＩＰアドレス、特定の送信元ＴＣＰポート番号、特定の送信先ＴＣＰポート番号、特定の送信元ＵＤＰポート番号または特定の送信先ＵＤＰポート番号に限定する）については、パケット中継装置１がオトリ端末装置４１へ誘導する。

【００８５】オトリ端末装置４１は、受け取ったパケットについて、パケット情報を詳細に解析し、不正アクセスパケットか否かを判別する。その結果、不正アクセスパケットの可能性が低い場合には、実施の形態４と同様にして、当該パケットを内部ネットワーク３０へ中継する。

【００８６】一方、　不正アクセスパケットである可能性が高い場合には、身代わり端末装置４２へ誘導する。これにより、通信の種別（送信元ＩＰアドレス、送信先ＩＰアドレス、送信元ＴＣＰポート番号、送信先ＴＣＰポート番号、送信元ＵＤＰポート番号または送信先ＵＤＰポート番号で分類される）により、セキュリティ管理のレベルを変えて管理することが可能となる。

【００８７】実施の形態７．図１１は、本発明の実施の形態７によるオトリ誘導システムの構成および動作の一例を示した図である。図中の１はパケット中継装置、２０は外部ネットワーク、３０は内部ネットワーク、４１はオトリ端末装置、４３はネットワーク監査装置である。

【００８８】　通常運用時、外部ネットワーク２０からのパケットは内部ネットワーク３０へ直接中継されると共に、すべての通信パケットはコピーされ、オトリ端末装置４１へも送信される。　パケットを受け取ったオトリ端末装置４１では、受け取ったパケット情報を解析し、特定の閾値を超える数の通信が発生していた場合、その通信情報を特定の送信元ＩＰアドレス、特定の送信先ＩＰアドレス、特定の送信元ＴＣＰポート番号、特定の送信先ＴＣＰポート番号、特定の送信元ＵＤＰポート番号または特定の送信先ＵＤＰポート番号で指定し、内部ネットワーク３０の監査に用いる。具体的には、ネットワーク監査装置４３上の監査プログラムから同様のパケットを発生させ、内部ネットワーク３０の抗堪性を測定する。

【００８９】実施の形態８．図１２は、本発明の実施の形態８によるオトリ誘導システムの構成および動作の一例を示した図である。オトリ端末装置４１は、侵入検知部（不図示）を備えている。例えば、ホスト型ＩＤＳ（侵入検知プログラム）が予めインストールされている。不正アクセスパケットを検出したオトリ端末装置４１は、直ちにセッションリセットパケットを送信して、外部ネットワーク２０および内部ネットワーク３０間での当該セッションを切断する。

【００９０】次に動作について説明する。　通常運用時、外部ネットワーク２０からのパケットは内部ネットワーク３０へ直接中継されると共に、すべての通信はコピーされオトリ端末装置４１へも送信される。　オトリ端末装置４１は、パケット中継装置から受け取ったパケットが不正アクセスである場合、当該セッションに対しては、送信元ＩＰアドレス、送信先ＩＰアドレス、送信元ＴＣＰポート番号、送信先ＴＣＰポート番号を指定して、セッションリセットパケットを送信し、セッションを切断することにより、不正アクセスにリアルタイム対処を可能とする。

【００９１】

【発明の効果】本発明によれば、不正アクセスに対するセキュリティ性を向上させ、不正アクセスへの対処を自動化し、あるいは、通信量の増大時に通信路の帯域を確保することができるパケット中継装置を提供することができる。また、２つの中継経路を用いて中継経路における帯域を制御するとともにセキュリティ性を向上させたパケット中継システムを提供することができる。さらに、セキュリティ性を向上させ、セキュリティレベルを変化させ、ネットワークの監査を行い、あるいは、不正アクセスへの対処をリアルタイム化したオトリ誘導システムを提供することができる。

【図面の簡単な説明】

【図１】　本発明の実施の形態１によるオトリ誘導システムの一構成例を示したブロック図である。

【図２】　図１のオトリ誘導システムにおけるパケットの流れの一例を示した図である。

【図３】　本発明の実施の形態２によるオトリ誘導システムの一構成例を示したブロック図である。

【図４】　図３のオトリ誘導システムの通常運用時の動作の一例を示した図である。

【図５】　図３のオトリ誘導システムにおいて、フィルタリング処理部によってパケットがオトリ誘導される場合の動作の一例を示した図である。

【図６】　本発明の実施の形態３によるオトリ端末装置から攻撃者以外の外部端末装置にパケット送信する場合の動作を示した説明図である。

【図７】　攻撃者以外の外部端末装置からオトリ端末装置４１に対してパケット送信する場合の動作を示した説明図である。

【図８】　本発明の実施の形態４によるオトリ誘導システムの動作の一例を示した説明図である。

【図９】　本発明の実施の形態５によるパケット中継システムの一構成例を示した図である。

【図１０】　本発明の実施の形態６によるオトリ誘導システムの構成および動作の一例を示した図である。

【図１１】　本発明の実施の形態７によるオトリ誘導システムの構成および動作の一例を示した図である。

【図１２】　本発明の実施の形態８によるオトリ誘導システムの構成および動作の一例を示した図である。

19

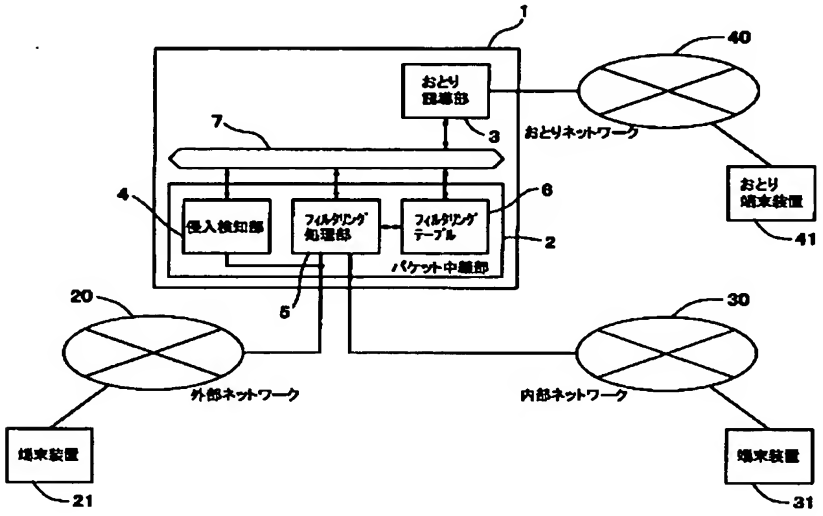
【図１３】　従来の侵入検知システムの構成および動作を示した図である。

【符号の説明】

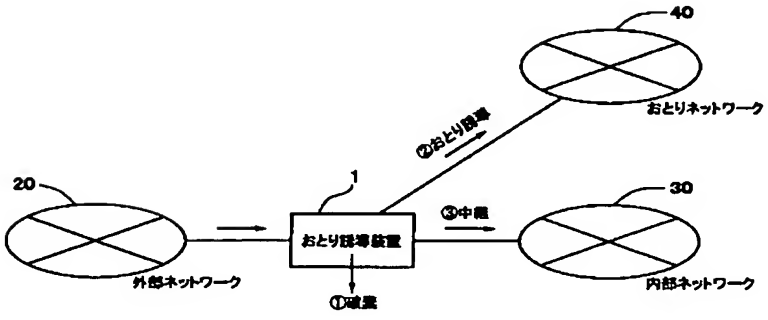
１　オトリ誘導装置（パケット中継装置）、１Ａ，１Ｂ　パケット中継装置、２　パケット中継部、３　オトリ誘導部、４　侵入検知部、５　フィルタリング処理部、６　フィルタリングテーブル、７　内部バス、８　パーソナルコンピュータ、９　アドインボード、１０　ＰＣＩバス、１１　ＰＣＩインターフェース部、１２　ＴＣＰ／ＩＰインターフェース部、１３　パケット中継システム、１４　パケット監視装置、１５　通常ルート、１６　監視ルート、２０　外部ネットワーク、２１　外部端末装置、３０　内部ネットワーク、３１　内部端末装置、４０　オトリネットワーク、４１　オトリ端末装置、４２　身代わり端末装置、４３　ネットワーク監査装置、５０　管理者端末装置、５１　解析装置

20

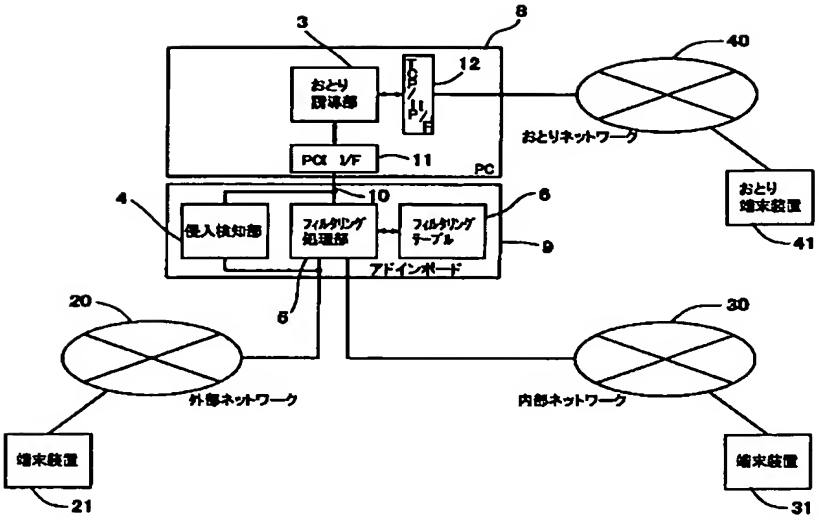
【図１】



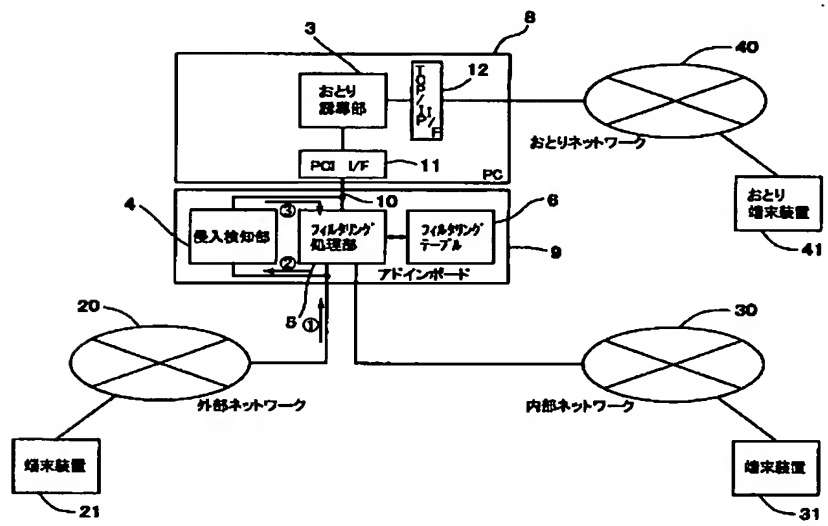
【図２】



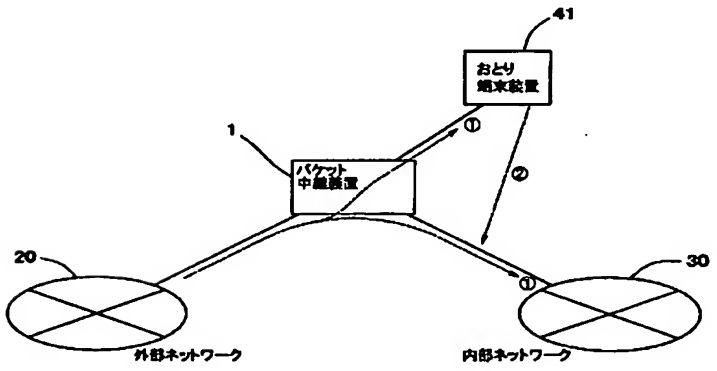
【図３】


3
8
12
40
おとり
誘導部
TCP/UDP/IP
おとりネットワーク
PCI I/F
11
PC
おとり
端末装置
41
4
10
6
侵入検知部
フィルタリング
処理部
フィルタリング
テーブル
9
アドインボード
5
20
30
外部ネットワーク
内部ネットワーク
端末装置
端末装置
21
31

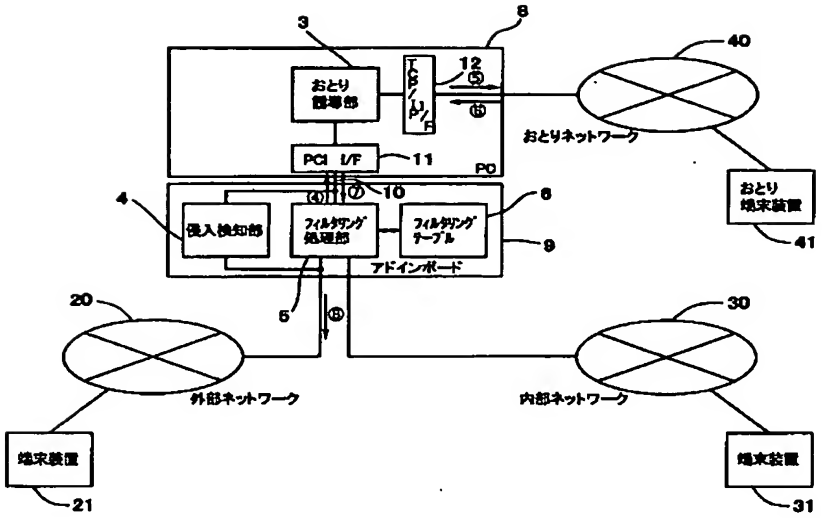
【図４】


3
8
12
40
おとり
誘導部
TCP/UDP/IP
おとりネットワーク
PCI I/F
11
PC
おとり
端末装置
41
4
③
10
6
侵入検知部
フィルタリング
処理部
フィルタリング
テーブル
9
②
アドインボード
5 ①
20
30
外部ネットワーク
内部ネットワーク
端末装置
端末装置
21
31

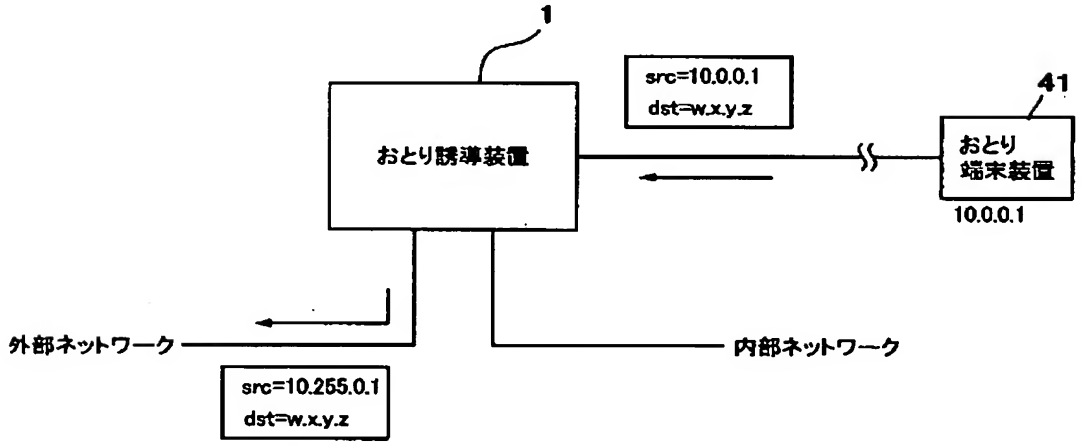
【図１２】


41
おとり
端末装置
①
1
パケット
中継装置
②
20
30
①
外部ネットワーク
内部ネットワーク

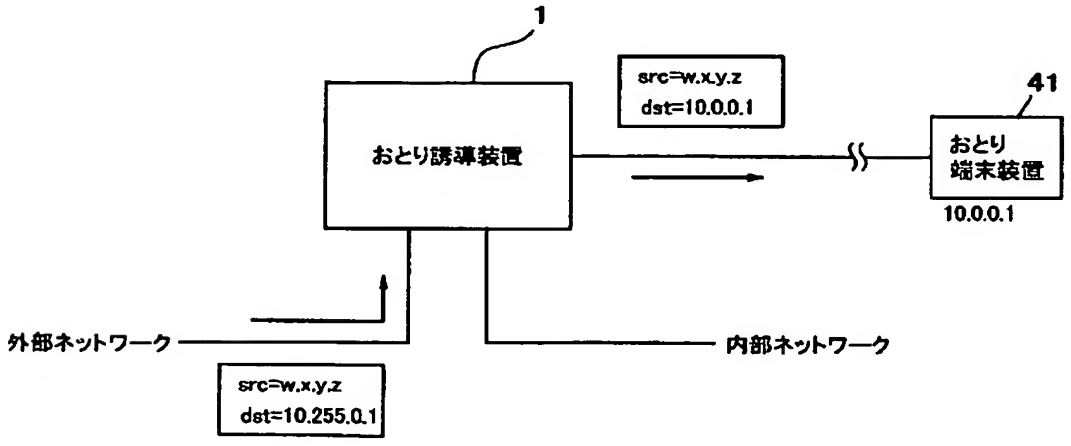
【図５】


3
8
40
おとり
誘導部
TCP/IP
I/F
12
⑤
⑥
おとりネットワーク
PCI I/F
11
PD
おとり
端末装置
41
4
10
侵入検知部
フィルタリング
処理部
フィルタリング
テーブル
6
9
アドインボード
5
⑮
20
30
外部ネットワーク
内部ネットワーク
端末装置
端末装置
21
31

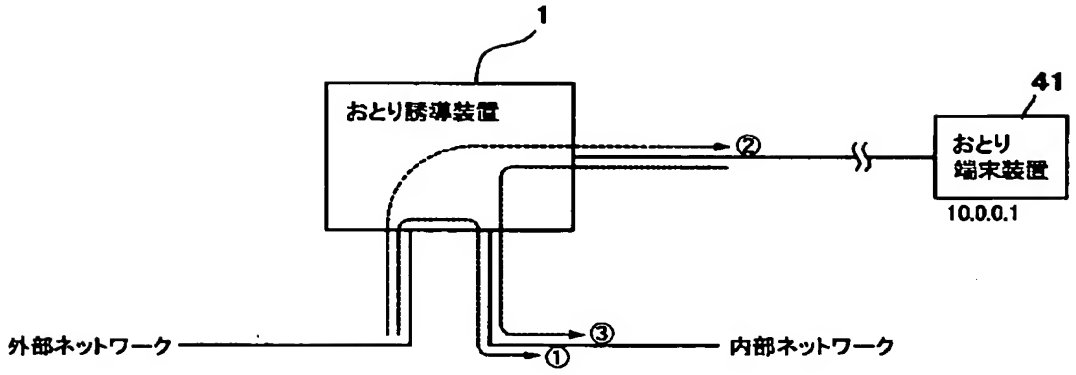
【図６】


1
src=10.0.0.1
dst=w.x.y.z
41
おとり誘導装置
おとり
端末装置
10.0.0.1
外部ネットワーク
内部ネットワーク
src=10.255.0.1
dst=w.x.y.z

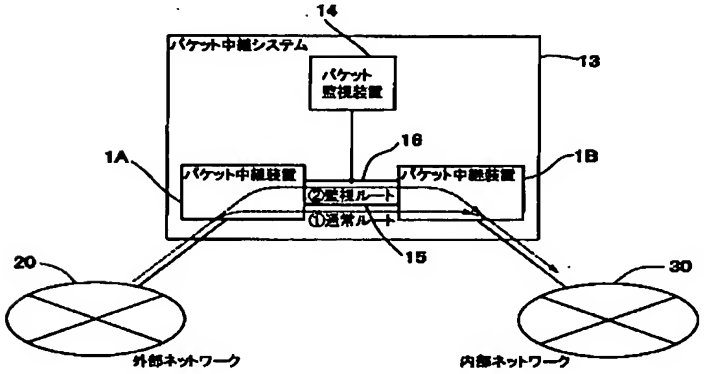
【図７】


1
src=w.x.y.z
dst=10.0.0.1
41
おとり誘導装置
おとり
端末装置
10.0.0.1
外部ネットワーク
内部ネットワーク
src=w.x.y.z
dst=10.255.0.1

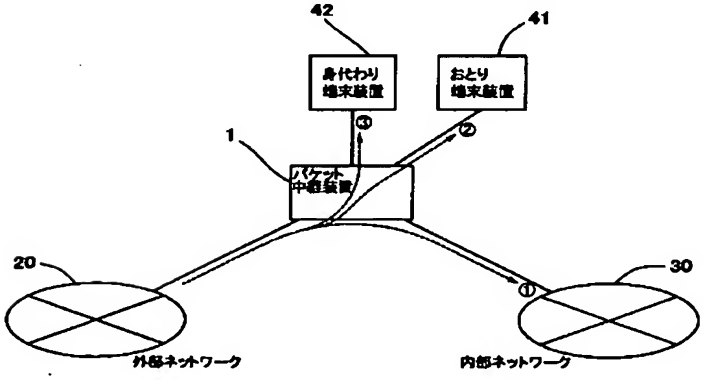
【図８】


1
おとり誘導装置
41
おとり
端末装置
10.0.0.1
②
③
①
外部ネットワーク
内部ネットワーク

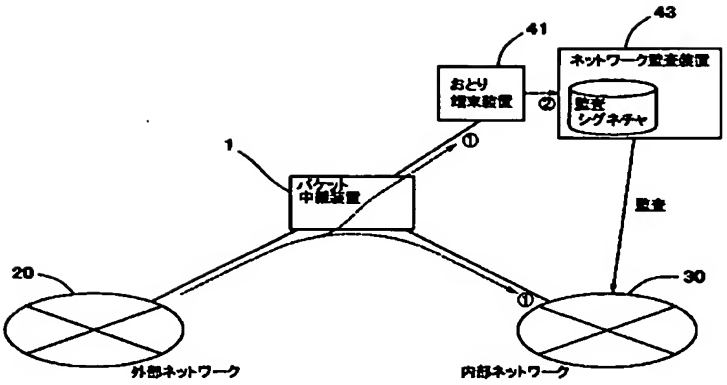
【図９】


14
パケット中継システム
パケット
監視装置
13
16
1A
1B
パケット中継装置
パケット中継装置
②変更ルート
①通常ルート
15
20
30
外部ネットワーク
内部ネットワーク

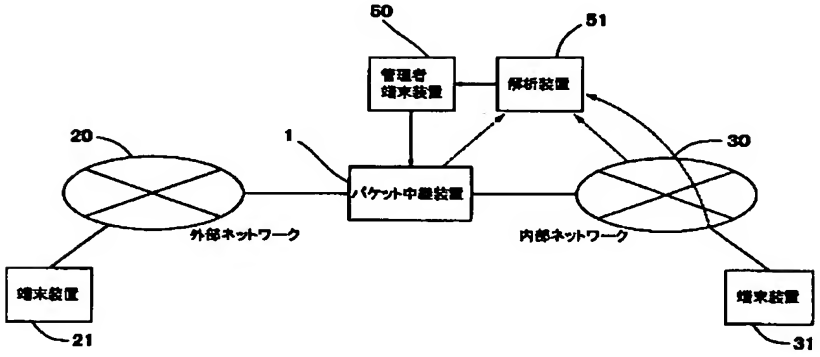
【図１０】


42
41
身代わり
端末装置
おとり
端末装置
③
②
1
パケット
中継装置
20
30
①
外部ネットワーク
内部ネットワーク

【図１１】


41
43
おとり
端末装置
ネットワーク監査装置
監査
シグネチャ
②
①
1
パケット
中継装置
監査
20
30
①
外部ネットワーク
内部ネットワーク

【図１３】


50
51
管理者
端末装置
解析装置
20
1
30
パケット中継装置
外部ネットワーク
内部ネットワーク
端末装置
端末装置
21
31